



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hisatoshi EGUCHI, et al.

GAU:

SERIAL NO: 10/685,399

EXAMINER:

FILED: October 16, 2003

FOR: SERVICE VERIFYING SYSTEM, AUTHENTICATION REQUESTING TERMINAL, SERVICE UTILIZING TERMINAL, AND SERVICE PROVIDING METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. _____ Date Filed _____

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

JAPAN

APPLICATION NUMBER

2002-302102

MONTH/DAY/YEAR

October 16, 2002

Certified copies of the corresponding Convention Application(s)

☒ are submitted herewith

- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. _____ filed _____
- ☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.
Masayasu Mori

Registration No. 47,301

Joseph A. Scafetta, Jr.
Registration No. 26,803

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2002年10月16日

出願番号
Application Number: 特願2002-302102
[ST. 10/C]: [JP2002-302102]

出願人
Applicant(s): 株式会社エス・ティ・ティ・ドコモ

2003年 9月26日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



CERTIFIED COPY OF
PRIORITY DOCUMENT

出証番号 出証特2003-307961

【書類名】 特許願

【整理番号】 14-0314

【提出日】 平成14年10月16日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 11 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 江口 悠利

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 11 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 三浦 史光

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】 100088155

【弁理士】

【氏名又は名称】 長谷川 芳樹

【選任した代理人】

【識別番号】 100092657

【弁理士】

【氏名又は名称】 寺崎 史朗

【選任した代理人】

【識別番号】 100114270

【弁理士】

【氏名又は名称】 黒川 朋也

【選任した代理人】

【識別番号】 100108213

【弁理士】

【氏名又は名称】 阿部 豊隆

【選任した代理人】

【識別番号】 100113549

【弁理士】

【氏名又は名称】 鈴木 守

【手数料の表示】

【予納台帳番号】 014708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 サービス検証システム、認証要求端末、サービス利用端末、サービス検証ネットワークシステム、及びサービス提供方法、

【特許請求の範囲】

【請求項 1】 複数のサービスを提供するサービス検証システムであって、
第 1 のサービスを利用可能なユーザを認証するための認証情報を格納した認証情報格納手段と、

それぞれのユーザが利用可能なサービスに関する情報を格納した利用可能サービス情報格納手段と、

前記第 1 のサービスとは異なる第 2 のサービスの利用を許可する際に、その利用許可を識別する利用許可メッセージを復元するためのメッセージ情報を格納する利用許可メッセージ情報格納手段と、

前記メッセージ情報が利用可能であるか否かを示すメッセージ状態情報を格納する利用許可メッセージ状態格納手段と、

第 1 の端末の認証方式に従ったメッセージを受信する第 1 メッセージ受信手段と、

前記第 1 メッセージ受信手段によって受信したメッセージを前記認証情報格納手段に格納された認証情報に基づいて検証することにより、前記第 1 の端末のユーザを特定すると共に前記ユーザが第 1 のサービスを利用可能か否かを認証する認証手段と、

前記認証手段によって第 1 のサービスを利用可能であると認証された前記第 1 の端末から送信される、第 2 のサービスの利用要求を受信する他サービス利用要求受信手段と、

前記他サービス利用要求受信手段によって前記利用要求を受信した際に、前記利用可能サービス情報格納手段の情報に基づいて、前記ユーザが前記第 2 のサービスを利用可能か否かを判定する他サービス利用可否判定手段と、

前記他サービス利用可否判定手段によって前記第 2 のサービスを利用可能と判定された場合に、前記利用許可メッセージ情報格納手段に第 2 のサービスの利用許可を識別する利用許可メッセージを復元するメッセージ情報を格納すると共に

、前記利用許可メッセージ状態格納手段に前記メッセージ情報が使用可能である状態を示すメッセージ状態情報を格納する利用許可メッセージ状態更新手段と、

前記他サービス利用可否判定手段によって前記第2のサービスの利用が可能であると判定された場合に、前記利用許可メッセージに基づく利用許可応答を前記第1の端末に送信する利用許可応答送信手段と、

第2の端末から送信される、前記利用許可応答に基づくメッセージを受信する第2メッセージ受信手段と、

前記利用許可メッセージ状態格納手段に格納されたメッセージ状態情報に基づいて、前記第2メッセージ受信手段で受信されたメッセージが利用可能であるか否かと共に、前記利用許可メッセージ情報格納手段に格納されたメッセージ情報に基づいて、前記メッセージの整合がとれているか否かを検証して、前記第2の端末に第2のサービスを提供可能か否かを判定するサービス提供可否判定手段と、

前記サービス提供可否判定手段により、第2のサービスを提供可能であると判定された場合には、第2のサービスの利用を許可し、前記利用許可メッセージ状態格納手段のメッセージ状態情報を使用可能でない状態にする利用許可メッセージ状態解除手段と、

を備えることを特徴とするサービス検証システム。

【請求項2】 第2のサービスを利用するために用いる追加情報にさらに基づくメッセージを検証するための追加情報を格納する追加情報格納手段と、

前記第2メッセージ受信手段において、さらに追加情報に基づくメッセージを受信し、

前記サービス提供可否判定手段において、前記追加情報格納手段に格納された追加情報にさらに基づいて、前記第2メッセージ受信手段で受信されたメッセージを検証して、第2のサービスが利用可能であるか否かを判定することを特徴とする請求項1に記載のサービス検証システム。

【請求項3】 第2のサービスを利用可能なエリアに関する利用可能エリア情報を格納するエリア情報格納手段と、

前記他サービス利用要求受信手段によって前記利用要求を受信した際に、前記第1の端末の在圏エリアに関する情報から利用可能エリア情報を導出し、前記利

用可能エリア情報を前記エリア情報格納手段に格納するエリア情報更新手段と、
を備え、

前記サービス提供可否判定手段は、前記第2の端末の在圏エリアが前記エリア情報格納手段に格納された利用可能エリア情報から導出されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、
ことを特徴とする請求項1又は2に記載のサービス検証システム。

【請求項4】 前記エリア情報更新手段は、前記利用可能メッセージ情報格納手段に格納されたメッセージ情報と、前記利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、前記第1の端末に送信した利用許可応答が基づいている前記利用許可メッセージが使用可能である状態と判明するとき、前記第1の端末の在圏エリアが前記エリア情報格納手段により判明する利用可能エリアの外に移動した場合には、前記第1の端末が移動した後の在圏エリアに関する情報から導出した利用可能エリア情報を前記エリア情報格納手段に格納することを特徴とする請求項3に記載のサービス検証システム。

【請求項5】 前記エリア情報更新手段は、前記利用可能メッセージ情報格納手段に格納されたメッセージ情報と、前記利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、前記第1の端末に送信した利用許可応答が基づいている前記利用許可メッセージが使用可能である状態と判明するとき、前記第1の端末の在圏エリアが前記エリア情報格納手段により判明する要求エリアの外に移動した場合に、前記他サービス利用要求受信手段によって利用要求を受信すると、前記第1の端末が移動した後の在圏エリアに関する情報から導出した利用可能エリア情報を前記エリア情報格納手段に格納することを特徴とする請求項3又は4に記載のサービス検証システム。

【請求項6】 第2のサービスを利用可能な時間に関する利用可能時間情報を格納する時間情報格納手段と、

前記他サービス利用要求受信手段によって前記利用要求を受信した際に、前記第2のサービスを利用できる利用可能時間情報を前記時間情報格納手段に格納する時間情報更新手段と、

をさらに備え、

前記サービス提供可否判定手段は、前記第2メッセージ受信手段によってメッセージを受信した時刻がサービスを利用可能な時間内に含まれるか、前記時間情報格納手段に格納された利用可能時間情報に基づいてさらに判定し、前記メッセージを受信した時刻が第2のサービスを利用可能な時間内に含まれる場合に第2のサービスを提供可能と判定する、

ことを特徴とする請求項1～5のいずれか1項に記載のサービス検証システム。

【請求項7】 前記利用許可応答送信手段は、前記第1の端末の在圏エリアに関する情報から導出された利用可能エリア情報にさらに基づく前記利用許可応答を送信し、

前記サービス提供可否判定手段は、前記第2の端末の在圏エリアが、前記メッセージに基づいている利用可能エリア情報で示されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、

ことを特徴とする請求項1～6のいずれか1項に記載のサービス検証システム。

【請求項8】 前記利用許可応答送信手段は、前記第2のサービスを利用可能な時間に関する利用可能時間情報にさらに基づく前記利用許可応答を送信し、

前記サービス提供可否判定手段は、前記第2メッセージ受信手段によってメッセージを受信した時刻が、前記メッセージに基づいている利用可能時間情報で示される時間内に含まれるか否かをさらに判定し、前記メッセージを受信した時刻が利用可能時間情報で示される時間内に含まれる場合に第2のサービスを提供可能と判定する、

ことを特徴とする請求項1～7のいずれか1項に記載のサービス検証システム。

【請求項9】 サービス検証システムによって提供される第1のサービスを利用できると共に第1のサービスの提供を受けるための認証を行う認証要求端末であって、

第1のサービスを利用するための認証情報を格納した認証情報格納手段と、
認証情報格納手段に格納された認証情報に基づいており、認証方式に従ったメ

ッセージを前記サービス検証システムに送信する第1メッセージ送信手段と、

前記サービス検証システムによって第1のサービスを利用可能と判定された場合に、第2のサービスの利用要求を送信する他サービス利用要求送信手段と、

前記他サービス利用要求送信手段によって送信された利用要求に応じて前記サービス検証システムから送信される、利用許可メッセージに基づく利用許可応答を受信する利用許可応答受信手段と、

を備えることを特徴とする認証要求端末。

【請求項10】 前記利用許可応答受信手段は、第2のサービスの利用可能エリア情報にさらに基づく利用許可応答を受信することを特徴とする請求項9に記載の認証要求端末。

【請求項11】 前記利用許可応答受信手段は、第2のサービスの利用可能時間情報にさらに基づく利用許可応答を受信することを特徴とする請求項9又は10に記載の認証要求端末。

【請求項12】 サービス検証システムによって提供される第1のサービスを利用可能な認証要求端末が、前記サービス検証システムによって第2のサービスが利用可能であるか否か判定された結果に基づいて、第2のサービスの提供を受けるサービス利用端末であって、

第2のサービスを利用するためのメッセージを前記サービス検証システムに送信する第2メッセージ送信手段を備え、

前記メッセージは、前記認証要求端末が前記サービス検証システムから受信した利用許可応答に基づくことを特徴とするサービス利用端末。

【請求項13】 第2のサービスを利用するために用いる追加情報を格納した追加情報格納手段を備え、

前記第2メッセージ送信手段で送信される前記メッセージは、前記追加情報格納手段に格納された追加情報にさらに基づくことを特徴とする請求項12に記載のサービス利用端末。

【請求項14】 複数のサービスを提供する請求項1又は3～6のいずれか1項に記載のサービス検証システムと、前記サービス検証システムによって提供される第1のサービスを利用する前記第1の端末としての請求項9に記載の認証

要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用する前記第2の端末としての請求項12に記載のサービス利用端末と、を備えることを特徴とするサービス検証ネットワークシステム。

【請求項15】 複数のサービスを提供する請求項1～6のいずれか1項に記載のサービス検証システムと、前記サービス検証システムによって提供される第1のサービスを利用する前記第1の端末としての請求項9に記載の認証要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用する前記第2の端末としての請求項13に記載のサービス利用端末と、を備えることを特徴とするサービス検証ネットワークシステム。

【請求項16】 複数のサービスを提供する請求項1又は3～7のいずれか1項に記載のサービス検証システムと、前記サービス検証システムによって提供される第1のサービスを利用する前記第1の端末としての請求項10に記載の認証要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用する前記第2の端末としての請求項12に記載のサービス利用端末と、を備えることを特徴とするサービス検証ネットワークシステム。

【請求項17】 複数のサービスを提供する請求項1～7のいずれか1項に記載のサービス検証システムと、前記サービス検証システムによって提供される第1のサービスを利用する前記第1の端末としての請求項10に記載の認証要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用する前記第2の端末としての請求項13に記載のサービス利用端末と、を備えることを特徴とするサービス検証ネットワークシステム。

【請求項18】 複数のサービスを提供する請求項1又は3～8のいずれか1項に記載のサービス検証システムと、前記サービス検証システムによって提供される第1のサービスを利用する前記第1の端末としての請求項11に記載の認証要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否

か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用する前記第2の端末としての請求項12に記載のサービス利用端末と、を備えることを特徴とするサービス検証ネットワークシステム。

【請求項19】 複数のサービスを提供する請求項1～8のいずれか1項に記載のサービス検証システムと、前記サービス検証システムによって提供される第1のサービスを利用する前記第1の端末としての請求項11に記載の認証要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用する前記第2の端末としての請求項13に記載のサービス利用端末と、を備えることを特徴とするサービス検証ネットワークシステム。

【請求項20】 複数のサービスを提供するサービス検証システムと、前記サービス検証システムによって認証され、前記サービス検証システムによって提供される第1のサービスを利用する認証要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用するサービス利用端末と、を備えるサービス検証ネットワークシステムにおいてサービスを提供するサービス提供方法であって、

前記認証要求端末が認証情報に基づき、認証方式に従ったメッセージを送信して前記サービス検証システムに受信させる第1メッセージ送信ステップと、

第1メッセージ送信ステップにおいて受信したメッセージを、前記サービス検証システムにあらかじめ格納された認証情報に基づいて検証することにより、前記認証要求端末のユーザを特定すると共に前記ユーザが第1のサービスを利用可能か否か認証する認証ステップと、

第1のサービスを利用可能であるときに、前記認証要求端末が第2のサービスの利用要求を送信して前記サービス検証システムに受信させる他サービス利用要求送信ステップと、

前記他サービス利用要求送信ステップにおいて前記利用要求を受信した際に、前記サービス検証システムが、ユーザが利用可能なサービスに関する情報があらかじめ格納された利用可能サービス情報格納手段に基づいて、前記ユーザが前記

第2のサービスを利用可能か否か判定する他サービス利用可否判定ステップと、

前記他サービス利用可否判定ステップにおいて前記第2のサービスを利用可能と判定された場合に、前記利用許可メッセージ情報格納手段に第2のサービスの利用許可を識別するための利用許可メッセージを復元するメッセージ情報を格納すると共に、前記利用許可メッセージ状態格納手段に前記メッセージ情報が使用可能である状態を示すメッセージ状態情報を格納する利用許可メッセージ状態更新ステップと、

前記他サービス利用可否判定ステップにおいて前記第2のサービスを利用可能と判定された場合に、前記サービス検証システムが利用許可メッセージに基づく利用許可応答を送信して前記認証要求端末に受信させる利用許可応答送信ステップと、

前記利用許可応答送信ステップにおいて前記認証要求端末が受信した利用許可応答に基づくメッセージを、前記サービス利用端末が送信して前記サービス検証システムに受信させる第2メッセージ送信ステップと、

前記利用許可メッセージ状態格納手段に格納されたメッセージ状態情報に基づいて、前記第2メッセージ受信ステップで受信されたメッセージが利用可能であるか否かと共に、前記利用許可メッセージ情報格納手段に格納されたメッセージ情報に基づいて前記メッセージの整合がとれているか否かを検証して、前記サービス利用端末に第2のサービスを提供可能か否か判定するサービス提供可否判定ステップと、

前記サービス提供可否判定ステップにより、第2のサービスを提供可能であると判定された場合には、第2のサービスの利用を許可し、前記利用許可メッセージ状態格納手段のメッセージ状態情報を使用可能でない状態にする利用許可メッセージ状態解除ステップと、

を有することを特徴とするサービス提供方法。

【請求項21】 前記第2メッセージ受信ステップにおいて、さらに追加情報に基づくメッセージを受信する機能を有し、

前記サービス提供可否判定手段において、追加情報格納手段に格納された追加情報にさらに基づいて、前記第2メッセージ受信ステップで受信されたメッセー

ジを検証して第2のサービスが利用可能であるか否かを判定することを特徴とする請求項20に記載のサービス提供方法。

【請求項22】 前記他サービス利用要求送信ステップにおいて前記利用要求を受信した際に、前記認証要求端末の在圏エリアに関する情報から利用可能エリア情報を導出して、前記利用可能エリア情報をエリア情報格納手段に格納するエリア情報更新ステップを有し、

前記サービス提供可否判定ステップは、前記サービス利用端末の在圏エリアが、前記エリア情報格納手段に格納された利用可能エリア情報で示されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、

ことを特徴とする請求項20又は21に記載のサービス提供方法。

【請求項23】 前記利用可能メッセージ情報格納手段に格納されたメッセージ情報と、前記利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、前記認証要求端末に送信した利用許可応答が基づいている前記利用許可メッセージが使用可能であると判明するとき、前記認証要求端末の在圏エリアが前記エリア情報格納手段により判明する利用可能エリアの外に移動した場合には、移動後での在圏エリアに関する情報から導出した利用可能エリア情報を前記エリア情報格納手段に格納する第2のエリア情報更新ステップを有することを特徴とする請求項22に記載のサービス提供方法。

【請求項24】 前記利用可能メッセージ情報格納手段に格納されたメッセージ情報と、前記利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、前記認証要求端末に送信した利用許可応答が基づいている前記利用許可メッセージが使用可能であると判明するとき、前記認証要求端末の在圏エリアが前記エリア情報格納手段により判明する利用可能エリアの外に移動した場合には、前記認証要求端末が第2のサービスの利用要求を送信して、前記他サービス利用要求受信ステップにおいて利用要求を受信すると、移動後での在圏エリアに関する情報から導出した利用可能エリア情報を前記エリア情報格納手段に格納する第2のエリア情報更新ステップを有することを特徴とする請求項22又は23に記載のサービス提供方法。

【請求項 25】 前記他サービス利用要求送信ステップにおいて前記利用要求を受信した際に、前記第2のサービスを利用できる利用可能時間情報を時間情報格納手段に格納する時間情報更新ステップを有し、

前記サービス提供可否判定ステップでは、前記第2メッセージ送信ステップにおいて前記サービス検証システムがメッセージを受信した時刻がサービス利用可能時間内に含まれるか、前記時間情報格納手段に格納された利用可能時間情報に基づいてさらに判定し、前記メッセージを受信した時刻がサービス利用可能時間内に含まれる場合に第2のサービスを提供可能と判定する、

ことを特徴とする請求項 20～24 のいずれか1項に記載のサービス提供方法

。 【請求項 26】 前記利用許可応答送信ステップでは、前記認証要求端末の在圏エリアに関する情報から導出された利用可能エリア情報にさらに基づく前記利用許可応答を送信し、

前記サービス提供可否判定ステップでは、前記サービス利用端末の在圏エリアが、前記第2メッセージ送信ステップにおいて前記サービス検証システムが受信したメッセージに基づいている利用可能エリア情報で示されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、

ことを特徴とする請求項 20～25 のいずれか1項に記載のサービス提供方法

。 【請求項 27】 前記利用許可応答送信ステップでは、前記第2のサービスの利用可能時間情報にさらに基づく前記利用許可応答を送信し、

前記サービス提供可否判定ステップでは、前記第2メッセージ送信ステップにおいて前記サービス検証システムがメッセージを受信した時刻が、前記メッセージに基づいている利用可能時間情報で示される時間内に含まれるか否かをさらに判定し、前記メッセージを受信した時刻が利用可能時間情報で示される時間内に含まれる場合に第2のサービスを提供可能と判定する、

ことを特徴とする請求項 20～26 のいずれか1項に記載のサービス提供方法

。 【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数のサービスを提供するサービス検証システム、このサービス検証システムによって認証され、サービス検証システムによって提供されるサービスを利用する認証要求端末、この認証要求端末の認証結果に基づいてサービス検証システムによって提供されるサービスを利用するサービス利用端末、これらの構成要素を有するサービス検証ネットワークシステム及びサービス提供方法に関する。

【0002】

【従来の技術】

従来から、移動通信などにおいて携帯電話やPHSにサービスを提供するシステムが知られている。このようなサービスを利用するためにはサービスを提供している会社と契約する必要がある。サービスを提供する会社の多くは、サービスを利用する契約を結んだユーザ（正規ユーザ）のみにサービスを提供し、契約していないユーザにはサービスを提供しない。このために、正規ユーザのみにサービスを利用させるための方式が必要であり、このような方式はすでに実現されている。

【0003】

現在、サービスを提供するサービス検証システムでは、正規ユーザの顧客情報を管理し、この顧客情報を用いてサービスの利用を要求するユーザが正規ユーザであるか否か認証し、認証結果が正しいときのみサービスの利用を許可する制御方式が用いられている。サービスを正規ユーザにのみ利用させるためには、このようなシステムを作り上げる必要がある。

【0004】

【非特許文献1】

Bruce Schneier, "APPLIED CRYPTOGRAPHY", John Wiley & Sons, Inc., 1996, pp. 52-56

【非特許文献2】

"NTT Docomo テクニカルジャーナル Vol.9 No.4", (株)電気通信協会,

2002年1月, pp. 34-43.

【非特許文献3】

Keiji Tachikawa, "W-CDMA MOBILE COMMUNICATIONS SYSTEM", John Wiley & Sons, Ltd, 2002, pp. 345-356

【0 0 0 5】

【発明が解決しようとする課題】

しかしながら、上述したシステムにおいては、あるサービスを提供している会社が別のサービスを提供しようとする場合に、契約者である正規ユーザにのみ接続させるためのシステムを最初から作り上げなければならないので、コストや設計時間が多くかかる。また、障害などによるサービス停止を防止するためにシステムの維持管理も必要となるが、システムが大きくなればなるほど管理コストは大きくなる傾向にある。このような点で上述のシステムには更なる改善の余地があった。

【0 0 0 6】

そこで、本発明は上記課題を解決し、コスト上昇を抑制することができるサービス検証システム、認証要求端末、サービス利用端末、サービス検証ネットワークシステム、及びサービス提供方法を提供することを目的とする。

【0 0 0 7】

【課題を解決するための手段】

本発明に係るサービス検証システムは、複数のサービスを提供するサービス検証システムであって、第1のサービスを利用可能なユーザを認証するための認証情報を格納した認証情報格納手段と、それぞれのユーザが利用可能なサービスに関する情報を格納した利用可能サービス情報格納手段と、第1のサービスとは異なる第2のサービスの利用を許可する際に、その利用許可を識別する利用許可メッセージを復元するためのメッセージ情報を格納する利用許可メッセージ情報格納手段と、メッセージ情報が利用可能であるか否かを示すメッセージ状態情報を格納する利用許可メッセージ状態格納手段と、第1の端末の認証方式に従ったメッセージを受信する第1メッセージ受信手段と、第1メッセージ受信手段によって受信したメッセージを認証情報格納手段に格納された認証情報に基づいて検証

することにより、第1の端末のユーザを特定すると共にユーザが第1のサービスを利用可能か否か認証する認証手段と、認証手段によって第1のサービスを利用可能であると認証された第1の端末から送信される、第2のサービスの利用要求を受信する他サービス利用要求受信手段と、他サービス利用要求受信手段によって利用要求を受信した際に、利用可能サービス情報格納手段の情報に基づいて、ユーザが第2のサービスを利用可能か否か判定する他サービス利用可否判定手段と、他サービス利用可否判定手段によって第2のサービスを利用可能と判定された場合に、利用許可メッセージ情報格納手段に第2のサービスの利用許可を識別する利用許可メッセージを復元するメッセージ情報を格納すると共に、利用許可メッセージ状態格納手段にメッセージ情報が使用可能である状態を示すメッセージ状態情報を格納する利用許可メッセージ状態更新手段と、他サービス利用可否判定手段によって第2のサービスの利用が可能であると判定された場合に、利用許可メッセージに基づく利用許可応答を第1の端末に送信する利用許可応答送信手段と、第2の端末から送信される、利用許可応答に基づくメッセージを受信する第2メッセージ受信手段と、利用許可メッセージ状態格納手段に格納されたメッセージ状態情報に基づいて、第2メッセージ受信手段で受信されたメッセージが利用可能であるか否かと共に、利用許可メッセージ情報格納手段に格納されたメッセージ情報に基づいて、メッセージの整合がとれているか否かを検証して、第2の端末に第2のサービスを提供可能か否か判定するサービス提供可否判定手段と、サービス提供可否判定手段により、第2のサービスを提供可能であると判定された場合には、第2のサービスの利用を許可し、利用許可メッセージ状態格納手段のメッセージ状態情報を使用可能でない状態にする利用許可メッセージ状態解除手段と、を備えることを特徴とする。

【0008】

このように本発明に係るサービス検証システムは、認証手段を備え、第1の端末から当該端末の認証方式に従ったメッセージが送信されると、そのメッセージによって第1の端末のユーザを特定すると共に第1の端末が第1のサービスを利用可能か否か認証する。そして、認証によって第1の端末のユーザが正規ユーザであることを認証した状態で、他サービス利用要求受信手段が第1の端末から送

信される第2のサービスの利用要求を受信すると、他サービス利用可否判定手段が、利用サービス情報格納手段に基づいて、そのユーザが第2のサービスを利用可能か判定する。このような構成により、第1の端末のユーザが正規のユーザであることが認証された状態で第2のサービスの利用可否を判定するので、第1のサービスの認証結果を利用して、第2のサービスについては認証を省略することができる。判定の結果、第2のサービスを利用可能であると判定された場合には、利用許可を識別する利用許可メッセージを復元するメッセージ情報を利用許可メッセージ情報格納手段に格納し、利用許可メッセージが使用可能であるメッセージ状態情報を格納すると共に、利用許可メッセージに基づく利用許可応答を第1の端末に送信する。そして、利用許可メッセージに基づくメッセージが第2の端末から送信された場合には、そのメッセージを第2メッセージ受信手段によって受信し、そのメッセージに基づいている利用許可メッセージが利用可能な状態であるか否かを利用許可メッセージ状態格納手段に基づいて検証し、さらに、利用許可メッセージ情報格納手段に格納されたメッセージ情報に基づいて、利用許可メッセージが正しく構成されているか否かを検証し、利用許可メッセージが利用可能な状態で、かつ利用許可メッセージ自体が正しく構成されている場合には第2の端末に対して第2のサービスを提供する。このようにサービス検証システムによって第2のサービスを利用可能と判定されたときには、利用許可メッセージに基づく利用許可応答を第1の端末に送信し、第2の端末は、第1の端末が受信した利用許可メッセージに基づくメッセージをサービス検証システムに送信することにより、サービス検証システムは第2の端末から送信されたメッセージに基づいている利用許可メッセージが利用可能な状態か否かを検証すれば、第2の端末のユーザを特定するまでもなく、第2の端末にサービスを提供可能か否かを判定することができる。以上のように、第2のサービスの利用に際して第1のサービスの認証結果を用いることにより、第2のサービスを提供する際にも新たな認証手段を最初から作り上げる必要はなく、コストや設計時間を削減することができる。第1の端末が受信した利用許可応答を第2の端末に知得させる方法は、どのような方法であっても良い。例えば、第1の端末から第2の端末に近距離無線によって送信することとしても良いし、第1の端末を見たユーザが第2の端末に手

入力しても良い。なお、第1の端末と第2の端末とは同一端末であっても良く、この場合には端末内部で利用許可応答を通信することができるので好ましい。

【0009】

上記サービス検証システムは、第2のサービスを利用するために用いる追加情報にさらに基づくメッセージを検証するための追加情報を格納する追加情報格納手段と、第2メッセージ受信手段において、さらに追加情報に基づくメッセージを受信し、サービス提供可否判定手段において、追加情報格納手段に格納された追加情報にさらに基づいて、第2メッセージ受信手段で受信されたメッセージを検証して、第2のサービスが利用可能であるか否かを判定することを特徴としても良い。

【0010】

このように追加情報をさらに用いることにより、セキュリティを向上させてより安全に第2のサービスを提供することができる。追加情報としては、例えば、第2の端末を識別する識別情報や、第2の端末を認証するための認証情報などが考えられる。

【0011】

上記サービス検証システムは、第2のサービスを利用可能なエリアに関する利用可能エリア情報を格納するエリア情報格納手段と、他サービス利用要求受信手段によって利用要求を受信した際に、第1の端末の在圏エリアに関する情報から利用可能エリア情報を導出し、利用可能エリア情報をエリア情報格納手段に格納するエリア情報更新手段と、を備え、サービス提供可否判定手段は、第2の端末の在圏エリアがエリア情報格納手段に格納された利用可能エリア情報から導出されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0012】

このように第2のサービスの利用要求を受信した際に、第1の端末の在圏エリアから第2のサービスを利用可能なエリア情報を導出し、利用可能エリア情報としてエリア情報格納手段に格納しておき、第2の端末から送信されたメッセージを受信したときに、第2の端末の在圏エリアが利用可能エリア内であるか否かを

エリア情報格納手段に基づいて判定して、第2のサービスの提供可否を判定する構成を採用することにより、許可されたエリアのみでしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができる。

【0013】

上記サービス検証システムにおいて、エリア情報更新手段は、利用可能メッセージ情報格納手段に格納されたメッセージ情報と、利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、第1の端末に送信した利用許可応答が基づいている利用許可メッセージが使用可能である状態と判明するとき、第1の端末の在圏エリアがエリア情報格納手段により判明する利用可能エリアの外に移動した場合には、第1の端末が移動した後の在圏エリアに関する情報から導出した利用可能エリア情報をエリア情報格納手段に格納することを特徴としても良い。

【0014】

このように認証された第1の端末が在圏エリアが移動したときには、エリア情報更新手段によって、エリア情報格納手段に格納された利用可能エリア情報を更新することにより、ユーザが移動している場合にも対応することが可能である。

【0015】

上記サービス検証システムは、エリア情報更新手段は、利用可能メッセージ情報格納手段に格納されたメッセージ情報と、利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、第1の端末に送信した利用許可応答が基づいている利用許可メッセージが使用可能である状態と判明するとき、第1の端末の在圏エリアがエリア情報格納手段により判明する要求エリアの外に移動した場合に、他サービス利用要求受信手段によって利用要求を受信すると、第1の端末が移動した後の在圏エリアに関する情報から導出した利用可能エリア情報をエリア情報格納手段に格納することを特徴としても良い。

【0016】

このように認証された第1の端末の在圏エリアが移動した後に、他サービス利用要求受信手段によって他サービス利用要求を受信したときの第1の端末の在圏

エリアから利用可能エリア情報を導出することにより、ユーザが移動している場合にも対応することが可能である。

【0017】

上記サービス検証システムにおいて、第2のサービスを利用可能な時間に関する利用可能時間情報を格納する時間情報格納手段と、他サービス利用要求受信手段によって利用要求を受信した際に、第2のサービスを利用できる利用可能時間情報を時間情報格納手段に格納する時間情報更新手段と、をさらに備え、サービス提供可否判定手段は、第2メッセージ受信手段によってメッセージを受信した時刻がサービスを利用可能な時間内に含まれるか、時間情報格納手段に格納された利用可能時間情報に基づいてさらに判定し、メッセージを受信した時刻が第2のサービスを利用可能な時間内に含まれる場合に第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0018】

このように第2のサービスを利用できる時間を利用可能時間情報として時間情報格納手段に格納しておき、第2の端末からメッセージが送信されたときに、メッセージの受信時刻が第2のサービスの利用可能時間内に含まれているか否かを判定して、第2のサービスの提供可否を判定する構成を採用することにより、許可された時間内でしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができる。なお、第2のサービスを利用できる時間の設定方法は、例えば、第1の端末に対して利用許可応答を送信してから何分間というように設定することもできるし、第2のサービスの種類に応じて設定することもできる。

【0019】

上記サービス検証システムにおいて、利用許可応答送信手段は、第1の端末の在圏エリアに関する情報から導出された利用可能エリア情報にさらに基づく利用許可応答を送信し、サービス提供可否判定手段は、第2の端末の在圏エリアが、メッセージに基づいている利用可能エリア情報で示されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0020】

このように第2のサービスの利用要求を受信した際に、第1の端末の在圏エリアから第2のサービスを利用可能なエリア情報を導出し、この利用可能エリア情報にさらに基づく利用許可応答を第1の端末に送信し、第2の端末からメッセージが送信されたときに、そのメッセージが基づいている利用可能エリア内に第2の端末が含まれているか否かを判定して、第2のサービスの提供可否を判定する構成を採用することにより、許可されたエリアのみでしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができると共に、サービス検証システムは利用可能エリアに関する情報を格納しない構成とできる。

【0021】

上記サービス検証システムにおいて、利用許可応答送信手段は、第2のサービスを利用可能な時間に関する利用可能時間情報にさらに基づく利用許可応答を送信し、サービス提供可否判定手段は、第2メッセージ受信手段によってメッセージを受信した時刻が、メッセージが基づいている利用可能時間情報で示される時間内に含まれるか否かをさらに判定し、メッセージを受信した時刻が利用可能時間情報で示される時間内に含まれる場合に第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0022】

このように第2のサービスを利用できる時間を利用可能時間情報にさらに基づく利用許可応答を第1の端末に送信し、第2の端末からメッセージが送信されたときに、そのメッセージが基づいている利用可能時間内に、当該メッセージの受信時刻が含まれているか否かを判定して、第2のサービスの提供可否を判定する構成を採用することにより、許可された時間内でしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができると共に、サービス検証システムは利用可能時間に関する情報を格納しない構成とできる。

【0023】

本発明に係る認証要求端末は、サービス検証システムによって提供される第1

のサービスを利用できると共に第1のサービスの提供を受けるための認証を行う認証要求端末であって、第1のサービスを利用するための認証情報を格納した認証情報格納手段と、認証情報格納手段に格納された認証情報に基づいており、認証方式に従ったメッセージをサービス検証システムに送信する第1メッセージ送信手段と、サービス検証システムによって第1のサービスを利用可能と判定された場合に、第2のサービスの利用要求を送信する他サービス利用要求送信手段と、他サービス利用要求送信手段によって送信された利用要求に応じてサービス検証システムから送信される、利用許可メッセージに基づく利用許可応答を受信する利用許可応答受信手段と、を備えることを特徴とする。

【0024】

このように第1のサービスを利用するための認証情報に基づくメッセージをサービス検証システムに送信して、サービス検証システムによって正規ユーザであることが認証された状態で、第2のサービスの利用要求を送信することによって、第2のサービスについては、第1のサービスの認証結果を利用して認証を省略することができる。そして、認証要求端末は利用許可応答受信手段を有し、利用許可メッセージに基づく利用許可応答を受信する。そして、この利用許可応答を第2の端末（サービス利用装置）に知得させれば、第2の端末が利用許可応答に基づくメッセージをサービス検証システムに送信し、サービス検証システムはそのメッセージに基づくことになる利用許可メッセージが使用可能な状態であるか検証でき、第2の端末によって独自の認証を行わなくても、第2のサービスを利用することができる。なお、認証要求端末自身が第2の端末の機能を有することとしても良く、その場合にも、第2のサービスの利用に際して認証を省略できるというメリットを享受できる。

【0025】

上記認証要求端末において、利用許可応答受信手段は、第2のサービスの利用可能エリア情報にさらに基づく利用許可応答を受信することを特徴としても良い。

【0026】

利用許可応答受信手段が、利用可能エリア情報にさらに基づく利用許可応答を

受信することにより、この利用許可応答に基づくメッセージをサービス検証システムに送信すれば、サービス検証システムはそのメッセージが基づいている利用可能エリア内に第2の端末が含まれているか判定することができる。これにより、第2のサービスの利用可能エリアを限定することで不正利用の機会を少なくして、セキュリティを向上させることができる。

【0027】

上記認証要求端末において、利用許可応答受信手段は、第2のサービスの利用可能時間情報にさらに基づく利用許可応答を受信することの特徴としても良い。

【0028】

利用許可応答受信手段が、利用可能時間情報にさらに基づく利用許可応答を受信することにより、この利用許可応答に基づくメッセージをサービス検証システムに送信すれば、サービス検証システムは、第2の端末からのメッセージ受信時刻がそのメッセージが基づいている利用可能時間内であるか判定することができる。これにより、第2のサービスの利用可能時間を限定することで不正利用の機会を少なくして、セキュリティを向上させることができる。

【0029】

本発明に係るサービス利用端末は、サービス検証システムによって提供される第1のサービスを利用可能な認証要求端末が、サービス検証システムによって第2のサービスが利用可能であるか否か判定された結果に基づいて、第2のサービスの提供を受けるサービス利用端末であって、第2のサービスを利用するためのメッセージをサービス検証システムに送信する第2メッセージ送信手段を備え、メッセージは、認証要求端末がサービス検証システムから受信した利用許可応答に基づくことを特徴とする。

【0030】

このように認証要求端末が受信した利用許可応答に基づくメッセージをサービス検証システムに送信することにより、サービス検証システムは送信されたメッセージが基づいている利用許可メッセージが使用可能な状態か否か判定できるので、サービス利用端末ではユーザの認証を省略して第2のサービスを利用することができる。

【0031】

上記サービス利用端末は、第2のサービスを利用するために用いる追加情報を格納した追加情報格納手段を備え、第2メッセージ送信手段で送信されるメッセージは、追加情報格納手段に格納された追加情報にさらに基づくことを特徴としても良い。

【0032】

このように追加情報をさらに用いることにより、セキュリティを向上させてより安全に第2のサービスを提供することができる。追加情報としては、例えば、サービス利用端末を識別する識別情報や、サービス利用端末を認証するための認証情報などが考えられる。

【0033】

本発明に係るサービス検証ネットワークシステムは、複数のサービスを提供する上記サービス検証システムと、サービス検証システムによって提供される第1のサービスを利用する第1の端末としての上記認証要求端末と、認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、サービス検証システムによって提供される第2のサービスを利用する第2の端末としての上記サービス利用端末と、を備えることを特徴とする。

【0034】

このような構成を採用することにより、サービス検証システムは、認証要求端末における認証結果を用いることで、サービス利用端末での認証を省略して第2のサービスを提供することができ、第2のサービスを提供する際に新たな認証手段を最初から作り上げる必要はなく、コストや設計時間を削減することができる。また、利用許可応答に利用可能なエリア情報や時間情報を含めることにより、利用可能なエリアや時間を限定して、不正利用の機会を少なくして、セキュリティを高めることができる。なお、認証要求端末とサービス利用端末とは同一端末であっても良い。

【0035】

本発明に係るサービス提供方法は、複数のサービスを提供するサービス検証システムと、前記サービス検証システムによって認証され、前記サービス検証シ

テムによって提供される第1のサービスを利用する認証要求端末と、前記認証要求端末によって第2のサービスが利用可能であるか否か判定された結果に基づいて、前記サービス検証システムによって提供される第2のサービスを利用するサービス利用端末と、を備えるサービス検証ネットワークシステムにおいてサービスを提供するサービス提供方法であって、前記認証要求端末が認証情報に基づき、認証方式に従ったメッセージを送信して前記サービス検証システムに受信させる第1メッセージ送信ステップと、第1メッセージ送信ステップにおいて受信したメッセージを、前記サービス検証システムにあらかじめ格納された認証情報に基づいて検証することにより、前記認証要求端末のユーザを特定すると共に前記ユーザが第1のサービスを利用可能か否か認証する認証ステップと、第1のサービスを利用可能であるときに、前記認証要求端末が第2のサービスの利用要求を送信して前記サービス検証システムに受信させる他サービス利用要求送信ステップと、前記他サービス利用要求送信ステップにおいて前記利用要求を受信した際に、前記サービス検証システムが、ユーザが利用可能なサービスに関する情報があらかじめ格納された利用可能サービス情報格納手段に基づいて、前記ユーザが前記第2のサービスを利用可能か否か判定する他サービス利用可否判定ステップと、前記他サービス利用可否判定ステップにおいて前記第2のサービスを利用可能と判定された場合に、前記利用許可メッセージ情報格納手段に第2のサービスの利用許可を識別するための利用許可メッセージを復元するメッセージ情報を格納すると共に、前記利用許可メッセージ状態格納手段に前記メッセージ情報が使用可能である状態を示すメッセージ状態情報を格納する利用許可メッセージ状態更新ステップと、前記他サービス利用可否判定ステップにおいて前記第2のサービスを利用可能と判定された場合に、前記サービス検証システムが利用許可メッセージに基づく利用許可応答を送信して前記認証要求端末に受信させる利用許可応答送信ステップと、前記利用許可応答送信ステップにおいて前記認証要求端末が受信した利用許可応答に基づくメッセージを、前記サービス利用端末が送信して前記サービス検証システムに受信させる第2メッセージ送信ステップと、前記利用許可メッセージ状態格納手段に格納されたメッセージ状態情報に基づいて、前記第2メッセージ受信ステップで受信されたメッセージが利用可能であるか否

かと共に、前記利用許可メッセージ情報格納手段に格納されたメッセージ情報に基づいて前記メッセージの整合がとれているか否かを検証して、前記サービス利用端末に第2のサービスを提供可能か否かを判定するサービス提供可否判定ステップと、前記サービス提供可否判定ステップにより、第2のサービスを提供可能であると判定された場合には、第2のサービスの利用を許可し、前記利用許可メッセージ状態格納手段のメッセージ状態情報を使用可能でない状態にする利用許可メッセージ状態解除ステップと、を有することを特徴とする。

【0036】

このように本発明に係るサービス提供方法は、認証要求端末から送信された認証要求端末の認証方式に従ったメッセージによって認証要求端末のユーザを特定すると共に認証要求端末が第1のサービスを利用可能か否か認証ステップにおいて認証する。そして、認証ステップにおいて認証要求端末のユーザが正規ユーザであることを認証した状態で、他サービス利用要求送信ステップにおいて、認証要求端末から送信される第2のサービスの利用要求を受信すると、他サービス利用可否判定ステップにおいて、利用サービス情報格納手段に基づいて、そのユーザが第2のサービスを利用可能かを判定する。このような構成により、認証要求端末のユーザが正規のユーザであることが認証された状態で第2のサービスの利用可否を判定することによって、第1のサービスの認証結果を利用して、第2のサービスについては認証を省略することができる。判定の結果、第2のサービスを利用可能であると判定された場合には、利用許可を識別する利用許可メッセージを復元するメッセージ情報を利用許可メッセージ情報格納手段に格納し、利用許可を識別する利用許可メッセージが利用可能である状態を示すメッセージ状態情報を格納すると共に、利用許可メッセージに基づく利用許可応答を認証要求端末に送信する。そして、第2メッセージ送信ステップにおいて、利用許可応答に基づく利用要求がサービス利用端末から送信された場合にはその利用要求を受信し、そのメッセージが基づいている利用許可メッセージが使用可能な状態であるか否かを利用許可メッセージ状態格納手段に基づいて検証し、さらに、利用許可メッセージ情報格納手段に格納されたメッセージ情報に基づいて、利用許可メッセージが正しく構成されているか否かを検証し、利用許可メッセージが使用可能な

状態で、かつ利用許可メッセージ自体が正しく構成されていると判定された場合にはサービス利用端末に対して第2のサービスを提供する。このように第2のサービスを利用可能と判定されたときには、利用許可メッセージに基づく利用許可応答に含めて認証要求端末に送信し、サービス利用端末は認証要求端末が受信した利用許可応答に基づくメッセージをサービス検証システムに送信することにより、サービス検証システムは、第2メッセージ送信ステップにおいて送信されたメッセージに基づいている利用許可メッセージの状態が使用可能な状態か否か判定すれば、サービス利用端末のユーザを特定するまでもなく、サービス利用端末にサービスを提供可能か否か判定することができる。以上のように、第2のサービスの利用に際して第1のサービスの認証結果を用いることにより、第2のサービスを提供する際に新たな認証手段を最初から作り上げる必要はなく、コストやシステム設計時間を削減することができる。認証要求端末が受信した利用許可応答をサービス利用端末に知得させる方法は、どのような方法であっても良い。例えば、認証要求端末からサービス利用端末に近距離無線によって送信することとしても良いし、認証要求端末を見たユーザがサービス利用端末に手入力しても良い。なお、認証要求端末とサービス利用端末とは同一端末であっても良く、この場合には端末内部で利用許可メッセージを通信することができるので好ましい。

【0037】

上記サービス提供方法は、第2メッセージ受信ステップにおいて、さらに追加情報に基づくメッセージを受信する機能を有し、サービス提供可否判定手段において、追加情報格納手段に格納された追加情報にさらに基づいて、第2メッセージ受信ステップで受信されたメッセージを検証して第2のサービスが利用可能であるか否か判定することを特徴としても良い。

【0038】

このように追加情報をさらに用いることにより、セキュリティを向上させてより安全に第2のサービスを提供することができる。追加情報としては、例えば、サービス利用端末を識別する識別情報や、サービス利用端末を認証するための認証情報などが考えられる。

【0039】

上記サービス提供方法は、他サービス利用要求送信ステップにおいて利用要求を受信した際に、認証要求端末の在圏エリアに関する情報から利用可能エリア情報を導出して、利用可能エリア情報をエリア情報格納手段に格納するエリア情報更新ステップを有し、サービス提供可否判定ステップは、サービス利用端末の在圏エリアが、エリア情報格納手段に格納された利用可能エリア情報で示されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0040】

このように他サービス利用要求送信ステップにおいて第2のサービスの利用要求をサービス検証システムが受信した際に、認証要求端末の在圏エリアから第2のサービスの利用可能エリアを導出して利用可能エリア情報としてエリア情報格納手段に格納し、第2メッセージ送信ステップにおいてサービス利用端末からメッセージが送信されたときにエリア情報格納手段に格納された利用可能エリア内にサービス利用端末が含まれているか否かを判定して、第2のサービスの提供可否を判定することにより、許可されたエリアのみでしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができる。

【0041】

上記サービス提供方法は、前記利用可能メッセージ情報格納手段に格納されたメッセージ情報と、前記利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、前記認証要求端末に送信した利用許可応答が基づいている前記利用許可メッセージが使用可能であると判明するとき、認証要求端末の在圏エリアがエリア情報格納手段により判明する利用可能エリアの外に移動した場合には、移動後での在圏エリアに関する情報から導出した利用可能エリア情報をエリア情報格納手段に格納する第2のエリア情報更新ステップを有することを特徴としても良い。

【0042】

このように認証された認証要求端末の在圏エリアが移動したときには、エリア情報格納手段に格納された利用可能エリア情報を更新することにより、ユーザが

移動している場合にも対応することが可能である。

【0043】

上記サービス提供方法は、前記利用可能メッセージ情報格納手段に格納されたメッセージ情報と、前記利用可能メッセージ状態格納手段に格納されたメッセージ状態情報を用いて、前記認証要求端末に送信した利用許可応答が基づいている前記利用許可メッセージが使用可能であると判明するとき、認証要求端末の在圏エリアがエリア情報格納手段により判明する利用可能エリアの外に移動した場合に、認証要求端末が第2のサービスの利用要求を送信して、他サービス利用要求受信ステップにおいて利用要求を受信すると、移動後での在圏エリアに関する情報から導出した利用可能エリア情報をエリア情報格納手段に格納する第2のエリア情報更新ステップを有することを特徴としても良い。

【0044】

このように認証された第1の端末の在圏エリアが移動した後に、他サービス利用要求受信ステップにおいて他サービス利用要求を受信したときの第1の端末の在圏エリアから利用可能エリア情報を導出することにより、ユーザが移動している場合にも対応することが可能である。

【0045】

上記サービス提供方法は、他サービス利用要求送信ステップにおいて利用要求を受信した際に、第2のサービスを利用できる利用可能時間情報を時間情報格納手段に格納する時間情報更新ステップを有し、サービス提供可否判定ステップでは、前記第2メッセージ送信ステップにおいて前記サービス検証システムがメッセージを受信した時刻がサービス利用可能時間内に含まれるか、時間情報格納手段に格納された利用可能時間情報に基づいてさらに判定し、メッセージを受信した時刻がサービス利用可能時間内に含まれる場合に第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0046】

このように第2のサービスを利用できる時間を利用可能時間情報として時間情報格納手段に格納し、第2メッセージ送信ステップにおいて第2の端末からメッセージが送信されたときに、メッセージの受信時刻が利用可能時間内に含まれて

いるか否かを判定して、第2のサービスの提供可否を判定することにより、許可された時間内でしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができる。なお、第2のサービスを利用できる時間の設定方法は、例えば、認証要求端末に対して利用許可応答を送信してから何分間というように設定することもできるし、第2のサービスの種類に応じて設定することもできる。

【0047】

上記サービス提供方法は、利用許可応答送信ステップでは、認証要求端末の在圏エリアに関する情報から導出された利用可能エリア情報にさらに基づく利用許可応答を送信し、サービス提供可否判定ステップでは、サービス利用端末の在圏エリアが、前記第2メッセージ送信ステップにおいて前記サービス検証システムが受信したメッセージが基づいている利用可能エリア情報で示されるエリア内であるか否かをさらに判定し、エリア内であれば第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0048】

このように第2のサービスの利用要求を受信した際に、第1の端末の在圏エリアから第2のサービスを利用可能なエリア情報を導出し、この利用可能エリア情報にさらに基づく利用許可応答を第1の端末に送信し、第2の端末からメッセージが送信されたときに、そのメッセージが基づいている利用可能エリア内に第2の端末が含まれているか否かを判定して、第2のサービスの提供可否を判定することにより、許可されたエリアのみでしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができると共に、サービス検証システムは利用可能エリアに関する情報を格納しない構成とできる。

【0049】

上記サービス提供方法は、利用許可応答送信ステップでは、第2のサービスの利用可能時間情報にさらに基づく利用許可応答を送信し、サービス提供可否判定ステップでは、第2メッセージ送信ステップにおいてサービス検証システムがメッセージを受信した時刻が、メッセージが基づいている利用可能時間情報で示さ

れる時間内に含まれるか否かをさらに判定し、メッセージを受信した時刻が利用可能時間情報で示される時間内に含まれる場合に第2のサービスを提供可能と判定する、ことを特徴としても良い。

【0050】

このように第2のサービスを利用できる時間を利用可能時間情報にさらに基づく利用許可応答を第1の端末に送信し、第2の端末からメッセージが送信されたときに、そのメッセージが基づいている利用可能時間内に、当該メッセージの受信時刻が含まれているか否かを判定して、第2のサービスの提供可否を判定することにより、許可された時間内でしか第2のサービスを利用できないことになり、不正利用の機会を少なくして、セキュリティを向上させることができると共に、サービス検証システムは利用可能時間に関する情報を格納しない構成とできる。

【0051】

【発明の実施の形態】

以下、図面と共に本発明に係るサービス検証ネットワークシステムの好適な実施形態について詳細に説明する。なお、図面の説明においては同一要素には同一符号を付し、重複する説明を省略する。

【0052】

(第1実施形態)

図1は、本発明の第1実施形態に係るサービス検証ネットワークシステム1の構成を示すブロック図である。図1に示されるように、サービス検証ネットワークシステム1は、サービス検証システム10と、認証要求端末30と、サービス利用端末40と、を有している。最初に各構成要素の概要を述べると、サービス検証システム10は、複数のサービスを提供する機能を有する。認証要求端末30は、サービス検証システム10によって提供されるサービスA(第1のサービス)を利用する端末であると共に、サービスAを利用するためにサービス検証システム10によって認証される端末である。サービス利用端末40は、サービス検証システム10によって提供されるサービスB(第2のサービス)を利用する端末である。本実施形態に係るサービス検証ネットワークシステム1において提

供されるサービスの一例としては、サービスAとして携帯電話、サービスBとして無線LANがあり、この場合には認証要求端末30として携帯電話端末、サービス利用端末40として無線LANカード付PCを想定することができる。なお、認証要求端末30とサービス利用端末40とは同一端末であっても良い。同一端末の例としては、例えば、一端で携帯電話とPHSが両方使用可能なドッチーモ（登録商標）を想定することができる。

【0053】

サービス検証システム10は、認証情報格納手段（「認証情報DB」という）11、利用可能サービス情報格納手段（「利用可能サービス情報DB」という）12、利用許可メッセージ状態格納手段（「利用許可メッセージ状態DB」という）13の3つのデータベースと、認証要求端末30及びサービス利用端末40のそれぞれと通信する通信手段14、15と、認証手段16と、他サービス利用可否判定手段17と、利用許可メッセージ状態更新手段18と、サービス提供可否判定手段19と、利用許可メッセージ状態解除手段20と、を備えている。ここでは、サービス検証システム10は一の装置によって構成されているが、複数の装置によって構成されていても良い。例えば、認証情報DB11、認証手段16、及び通信手段14によって構成される第1の装置と、利用可能サービス情報DB12、他サービス利用可否判定手段17、通信手段14、利用許可メッセージ状態更新手段18、及び利用許可メッセージ状態DB13によって構成される第2の装置と、サービス提供可否判定手段19、通信手段15、及び利用許可メッセージ状態更新手段20によって構成される第3の装置と、に分けられていても良い。

【0054】

認証情報DB11は、サービスAを利用可能なユーザを認証するための認証情報を格納したデータベースである。図2は認証情報DB11に格納されたデータ項目の例を示す図である。図2に示されるように、認証情報DB11には、「ID」「パスワード」「シェアードシークレット」「秘密鍵」「公開鍵」「認証方法」で示される項目のデータが格納される。なお、「ID」以外の項目については、データの内容の記載を省略している。「ID」は、サービスAを利用するユ

ーザを特定するための識別情報である。「パスワード」「シェアードシークレット」「秘密鍵」「公開鍵」の各情報は、認証を行うために必要な情報である。「認証方法」は、どのような方法で認証するかを表す情報であり、この情報を有することにより、ユーザに応じて認証の方法を変えることができる。なお、認証情報DB11には、図2に示したデータ項目以外の項目のデータを格納することとしても良い。

【0055】

利用可能サービス情報DB12は、それぞれのユーザが利用可能なサービスに関する情報を格納したデータベースである。図3は利用可能サービス情報DB12に格納されたデータ項目の例を示す図である。図3に示されるように、利用可能サービス情報DB12には、「ID」「サービスB」で示される項目のデータが格納される。「ID」は、認証情報DB11におけるIDと同じくユーザを特定するための識別情報である。「サービスB」は、サービス検証システム10によって提供されるサービスAと異なるサービスである。ここでは、サービスBについての情報を有するが、この項目はサービス検証システム10が提供するサービスが他にもあれば、その数に応じて利用可能サービス情報DB12に格納される項目は増減する。図3を参照すると、IDがU100のユーザは、サービスA以外にサービスBを利用可能であり、IDがU101のユーザはサービスBを利用できないことが分かる。

【0056】

利用許可メッセージ状態DB13は、サービスAとは異なるサービスBの利用を許可する際に、その利用許可を識別する利用許可メッセージのメッセージ状態情報を格納するデータベースである。図4は、利用許可メッセージ状態DB13に格納されたデータ項目の例を示す図である。図4に示されるように、利用許可メッセージ状態DB13は、「利用許可ID」「状態」で示される項目のデータが格納されている。「利用許可ID」は、利用許可メッセージを特定するための識別情報である。あるユーザにサービスBの利用を許可したことを識別する。利用許可IDは、利用許可メッセージ自体であっても良く、ここでは利用許可IDは利用許可メッセージであるとする。「状態」は、その利用許可IDで示される

サービスBを利用可能か否かを示す情報である。なお、複数のサービスを提供する場合には、利用許可メッセージ状態DB13は、それぞれのサービス毎に図4に示されるようなテーブルを有することとなる。本実施形態に係る利用許可メッセージ状態DB13は、利用許可ID（利用許可メッセージ）を格納しており、利用許可メッセージを復元するメッセージ情報を格納する利用許可メッセージ情報格納手段としての役割を有している。ここでは、利用許可メッセージ状態情報DB13に利用許可メッセージとメッセージ状態情報とを一緒に格納しているが、これらの情報を別々に格納する格納手段を有する構成としても良い。利用許可メッセージとメッセージ状態情報とを分離して格納した場合には、例えば、利用許可IDによって2つの情報を関連付けることができる。

【0057】

通信手段14は、認証要求端末30との通信を行う機能を有する。具体的には、通信手段14は、1) 認証要求端末30から送信される認証情報を受信する第1メッセージ受信手段としての機能、2) 認証要求端末30に認証結果を送信する認証結果送信手段としての機能、3) 認証要求端末30から送信されるサービスBの利用要求を受信する他サービス利用要求受信手段としての機能、4) サービスBを利用可能である場合に認証要求端末30に利用許可応答を送信する利用許可応答送信手段としての機能、などを有する。

【0058】

通信手段15は、サービス利用端末40との通信を行う機能を有する。具体的には、この通信手段15は、1) サービス利用端末40から送信されるサービスBの利用要求を受信する第2メッセージ受信手段としての機能、2) サービス利用端末40にサービスを提供する機能、などを有する。なお、サービス利用端末40から送信されるサービスの利用要求のメッセージは、認証要求端末30が受信した利用許可応答に基づいている。ここでは、認証要求端末30及びサービス利用端末40のそれぞれと通信する2つの通信手段14、15を有する構成を採用しているが、認証要求端末30とサービス利用端末40との通信プロトコルが同じ場合には、1つの通信手段によってそれぞれの端末30、40と通信することも可能である。

【0059】

認証手段16は、通信手段14によって認証要求端末30から受信したメッセージを用いて、認証要求端末30のユーザを特定すると共にユーザがサービスAを利用可能か否か認証する機能を有する。認証手段16は、認証情報DB11と接続されており、認証情報DB11に格納された認証情報に基づいて、認証要求端末30から受信したメッセージに含まれる認証情報を検証し、メッセージを送信した認証要求端末30のユーザが正規のユーザであるか否かを認証する。ここでの認証は、ID及びパスワードの照合を行う方法や公開鍵暗号方式などを採用することができる。正規のユーザであることが認証されると、そのユーザはサービス検証システム10が提供するサービスAを認証要求端末30によって利用可能となる。

【0060】

他サービス利用可否判定手段17は、認証要求端末30から送信される他サービスの利用要求を通信手段14によって受信した際に、認証要求端末30のユーザがそのサービスを利用できるか否か判定する機能を有する。他サービス利用可否判定手段17は、利用可能サービス情報DB12と接続されており、他サービスの利用要求が送信された際に、利用可能サービス情報DB12を参照して認証要求端末30のユーザが当該サービスを利用可能なサービスか否か判定する。例えば、図3に示す利用可能サービス情報DB12の場合には、ユーザIDがU101と認証された認証要求端末30からサービスBの利用要求を受信した場合には、他サービス利用可否判定手段17は利用不可能と判定することとなる。

【0061】

利用許可メッセージ状態更新手段18は、利用許可メッセージ状態DB13を更新する機能を有する。具体的には、他サービス利用可否判定手段17によって他のサービスを利用可能と判定された場合に、その利用許可にID（利用許可ID）を与え、そのIDを新たに追加する形式で更新する。なお、このときの「状態」は利用可能（図3では「○」で示される）となる。

【0062】

サービス提供可否判定手段19は、サービス利用端末40から受信したサービ

ス利用要求を通信手段14によって受信した際に、サービス利用端末40にサービスBを提供可能か否か判定する機能を有する。サービス提供可否判定手段19は、利用要求メッセージに基づいている利用許可メッセージのメッセージ状態情報を利用許可メッセージ状態DB13に基づいて検証することにより、そのサービスを提供可能か否かを判定し、利用許可メッセージの状態が使用可能である場合には、サービスBを提供可能と判定される。

【0063】

利用許可メッセージ状態解除手段20は、サービス利用端末40からメッセージが送信され、サービス提供可否判定手段19によってサービスを提供可能であると判定された場合に、利用許可メッセージの状態を使用可能な状態から使用できない状態に更新する機能を有する。すなわち、一旦、利用許可メッセージを含む利用要求を受信して他のサービスを提供した場合には、使用不可能（図3では「×」で示される）に更新する。このように一の利用メッセージを用いた利用要求を複数回受け付けないこととすれば、もし利用許可メッセージが第三者に知られたとしても、第三者に悪用される危険を低減することができる。

【0064】

次に、本実施形態に係る認証要求端末30について説明する。本実施形態に係る認証要求端末30は図1に示されるように、認証情報格納手段（「認証情報DB」という）31と、第1メッセージ送信手段33と、認証結果受信手段34と、他サービス利用要求送信手段35と、利用許可応答受信手段36と、通信手段32とを有する。

【0065】

認証情報DB31は、第1のサービスを利用するための認証情報を格納したデータベースであり、格納されるデータの項目は、サービス検証システム10が有する認証情報DB11と同じである（図2参照）。

【0066】

第1メッセージ送信手段33は、認証情報DB31に格納された認証情報を抽出してサービス検証システム10に認証のためのメッセージを送信する機能を有する。認証情報DB31から抽出される情報は、認証方法によって異なり、例え

パスワードによって認証を行う場合には、IDとパスワードと認証方法とが抽出され、秘密鍵方式で認証を行う場合には、IDと秘密鍵と認証方法とが抽出されて所定のメッセージが秘密鍵によって暗号化される。いずれの場合においても、認証方法に関する情報は、認証要求端末30とサービス検証システム10との間で認証方法の同期をとるために必要な情報である。

【0067】

認証結果受信手段34は、サービス検証システム10から送信される認証結果を受信する機能を有する。

【0068】

他サービス利用要求送信手段35は、サービスBの利用要求を送信する機能を有する。他サービス利用要求送信手段35は、認証結果受信手段34によって受信した認証結果に基づいて、サービスAを利用可能と判定された場合に、サービスBの利用要求を送信する。

【0069】

利用許可応答受信手段36は、サービス検証システム10から送信される利用許可メッセージに基づく利用許可応答を受信する機能を有する。

【0070】

通信手段14は、サービス検証システム10と通信する機能を有する。

【0071】

次に、本実施形態に係るサービス利用端末40について説明する。サービス利用端末40は図1に示されるように、第2メッセージ送信手段41と、通信手段42と、を有する。

【0072】

第2メッセージ送信手段41は、認証されたサービスAと異なるサービスBの利用を要求するメッセージを作成し、送信する機能を有する。第2メッセージ送信手段41は、認証要求端末30が利用許可応答受信手段36によって受信した利用許可応答に基づいてメッセージを作成する。例えば、利用許可応答を所定の関数によって処理することによって利用要求のメッセージを作成することができる。このような方式では、認証要求端末30やサービス利用端末40において、

利用許可メッセージが明らかにならないので、情報が遺漏する危険を低減させることができる。なお、認証要求端末30からサービス利用端末40に利用許可応答を伝達する方法は、任意の方法を採用できる。例えば、認証要求端末30とサービス利用端末40とを近距離無線によって通信可能としたり、ケーブルによって接続したりしても良い。また、認証要求端末30のディスプレイ上に表示された利用許可メッセージをサービス利用端末40に入力することによって伝達しても良い。

【0073】

次に、本実施形態に係るサービス検証ネットワークシステム1の動作について図5及び図6を参照しながら説明し、併せて、実施形態に係るサービス提供方法について説明する。

【0074】

最初に、認証要求端末30は、サービスAを利用するための認証を行う（S10）。認証処理の詳細について、図6を参照して説明する。まず、認証要求端末30は、サービス検証システム10に認証情報に基づくメッセージを送信する（S11）。サービス検証システム10は、認証要求端末30から送信されたメッセージを受信する（S12）と、受信したメッセージに基づいて認証処理を行う（S13）。サービス検証システム10は、認証要求端末30から送信されたメッセージから認証情報を解析し、認証情報DB11に格納された認証情報に基づいて認証要求端末30の認証を行う。認証処理が完了すると、サービス検証システム10は認証結果を認証要求端末30に送信する（S14）。ここでは、認証要求端末30のユーザが正規のユーザであり、サービスAを利用可能と認証されたものとするが、認証要求端末30のユーザが正規のユーザと認証されない場合には、認証要求端末30はサービスAを利用できない。認証要求端末30は、サービス検証システム10から送信された認証結果を受信する（S15）。認証要求端末30が受信した認証結果が、正しく認証されたことを示すものである場合には、認証要求端末30はサービスAを利用できる。ここまでのフローは、従来からのサービス検証ネットワークシステムと同じであり、所定のサービスを利用するためにユーザの認証を行っている。

【0075】

再び、図5を参照する。次に、認証要求端末30は、サービスAと異なるサービスBの利用要求をサービス検証システム10に送信する(S20)。サービス検証システム10は、認証要求端末30から送信される他サービス利用要求を受信する(S22)と、認証要求端末30のユーザがサービスBを利用可能であるか否かを判定する(S24)。具体的には、契約等によって認証要求端末30のユーザが利用可能となっているサービスに関する情報を格納した利用可能サービス情報DB12に基づいて、サービスBを利用可能かを判定する。なお、認証処理によってユーザは特定されているので、利用可能サービス情報DB12から利用可能なサービスの情報を抽出することができる。例えば、ユーザIDがU100のユーザの場合には、サービスBを利用可能と判定される(図3参照)。ここでは、サービスBを利用可能と判定されたものとする。サービスBを利用可能と判定されると、サービス検証システム10は、このユーザに対するサービスBの利用許可を識別する利用許可ID(利用許可メッセージ)を与え、利用許可メッセージ状態DB13を更新する(S26)。例えば、図4に示される利用許可メッセージ状態DB13において第3行目の「A102」が新しい利用許可メッセージとして追加されたとする。利用許可メッセージは、最初、使用可能(図4では「○」で示す)の状態を追加される。

【0076】

次に、サービス検証システム10は、利用要求に係るサービスBについての利用許可応答を認証要求端末30に送信する(S28)。認証要求端末30は利用許可応答を受信する(S30)と、受信した利用許可応答をサービス利用端末40に伝達する。本実施形態においては、認証要求端末30はサービス利用端末40との間で無線通信可能であるとし、認証要求端末30がサービス利用端末40に無線によって利用許可応答を送信し(S32)、サービス利用端末40が利用許可応答を受信するものとする(S34)。

【0077】

サービス利用端末40は、認証要求端末30から送信された利用許可応答を受信する(S34)と、利用許可応答に基づいてサービスBの利用を要求するメッ

セージを作成し、サービス利用端末40は、作成したメッセージをサービス検証システム10に送信する(S36)。サービス検証システム10は、サービス利用端末40から送信されたメッセージを受信し(S38)、受信したメッセージに基づいている利用許可メッセージを解析し、利用許可メッセージ状態DB13からメッセージ状態情報を検索する(S40)。続いて、受信したメッセージに基づいている利用許可メッセージが使用可能な状態か否か、さらに受信したメッセージ自体が正しく構成されているか否かの整合性を判定し、サービス提供可能か否かを判定する(S46)。例えば、利用要求から抽出した利用許可メッセージが「A102」であるとする、利用許可メッセージ状態DB13によれば、その状態は「○」であるので使用可能と判定され、サービス検証システム10はサービス利用端末40に対してサービスを提供可能である。サービスを提供可能である場合には、利用許可メッセージ状態解除手段20は利用許可メッセージ状態DB13に格納された利用許可メッセージの状態を使用可能な状態から使用できない状態にし、サービスBの利用可能状態を解除する。

【0078】

次に、サービス検証システム10は利用許可応答をサービス利用端末40に送信し(S48)、サービス利用端末40はサービス提供端末から送信された利用許可応答を受信し(S50)、サービスBを利用することが可能となる。以上で、本実施形態に係るサービス検証ネットワークシステム1の動作フローは終了する。

【0079】

本実施形態に係るサービス検証システム10(サービス検証ネットワークシステム1)は、サービスAを利用可能か否か判定する認証手段16と、他サービス利用可否判定手段17と、利用許可メッセージ状態DB13とを備え、認証手段16によってユーザを特定すると共にサービスAを利用可能とした状態で、サービスBを利用可能か否か判定する。これにより、サービスBの利用については、認証を要しないで利用可能か否か判定できる。また、サービスBを利用可能と判定された場合には、その利用許可に利用許可メッセージが使用可能であるというメッセージ状態情報を利用許可メッセージ状態DB13に格納すると共に、利用

許可メッセージに基づく利用許可応答を認証要求端末30に送信する。これにより、サービス検証システム10は、当該利用許可応答に基づくメッセージが送信された場合には、認証なしでそのメッセージを送信したサービス利用端末40にサービスBを提供することができる。従って、サービスAを提供するサービス検証システム10において、新たなサービスBを提供する場合に、サービスBを利用可能なユーザを認証する認証手段16を新たに構築しなくても、サービスAの認証手段16による認証結果を利用することで、低コストかつ短時間でサービス検証システム10を準備することができる。

【0080】

また、本実施形態に係るサービス提供方法は、認証処理によって認証要求端末30のユーザを特定すると共にサービスAを利用可能とした状態で、サービスBの利用要求を受信し、サービスBの利用判定を行うので、特定されたユーザがサービスBを利用可能か否かに判定するのみで良く、新たな認証を必要としない。そして、サービスBを利用可能と判定された場合には、その利用許可に利用許可メッセージを与えて使用可能であるというメッセージ状態情報を利用許可メッセージ状態DB13に格納すると共に、利用許可メッセージに基づく利用許可応答を認証要求端末30に送信する。これにより、本サービス提供方法では、当該利用許可メッセージを含む利用要求が送信された場合には、認証なしでその利用要求を送信したサービス利用端末40にサービスBを提供することができる。従って、サービスAを提供するサービス検証システム10において、新たなサービスBを提供する場合に、サービスBを利用可能なユーザを認証する認証手段16を新たに構築しなくても、サービスAの認証手段16による認証結果を利用することで、低コストかつ短時間でサービス検証システム10を準備することができる。

【0081】

(第2実施形態)

次に、本発明の第2実施形態に係るサービス検証ネットワークシステムについて説明する。第2実施形態に係るサービス検証ネットワークシステムは、第1実施形態に係るサービス検証ネットワークシステムと基本的な構成は同じであるが、サービス検証システム10aの構成が異なる。図7は、第2実施形態に係るサ

ービス検証システム10aの構成を示すブロック図である。図7に示されるように、第2実施形態に係るサービス検証システム10aは、第1実施形態に係るサービス検証システム10の構成に加え、エリア情報格納手段（「エリア情報DB」という）22、エリア情報更新手段21、時間情報格納手段（「時間情報DB」という）24、時間情報更新手段23、をさらに備えている。

【0082】

エリア情報DB22は、第2のサービスを利用可能なエリアに関する利用可能エリア情報を格納するデータベースである。図8は、エリア情報DB22に格納されたデータの例を示す図である。エリア情報DB22には、「利用許可ID」「利用可能エリア」の各情報が格納されている。「利用許可ID」は、利用許可メッセージを特定するための識別情報であり、利用許可メッセージ状態DB13に格納されたものと同じである。「利用可能エリア」は、第2のサービスを利用できるエリアに関する情報であり、サービス利用端末40が利用可能エリア内に存在しなければ、サービスを提供しない。ここでは、利用可能エリア情報は、利用許可IDに関連付けられているが、必ずしもこのようなデータ構造とする必要はなく、例えば認証要求端末30の識別情報などと関連付けて格納することとしても良いし、また他の情報とは独立して格納しても良い。

【0083】

エリア情報更新手段21は、エリア情報DB22を更新する機能を有する。エリア情報更新手段21は、他サービス利用可否判定手段17によってサービスBが利用可能と判定された場合に、その利用要求を送信した認証要求端末30の在圏エリアからサービスBを利用可能とする利用可能エリアを導出する。例えば、認証要求端末30の在圏エリアを含むエリアを利用可能エリアとすることもできるし、認証要求端末30の在圏エリアの一部を利用可能エリアとすることもできる。もちろん、認証要求端末30の在圏エリアと利用可能エリアが一致しても良い。そして、導出された利用可能エリア情報をエリア情報DB22に格納する。また、すでに他サービスの利用が許可されて利用許可メッセージ状態DB13に格納されたメッセージ状態情報が使用可能となっている認証要求端末30が移動して、その在圏エリアが変わった場合には、認証要求端末30から再度他サービ

ス利用要求が送信されるが、この際にも認証要求端末30の在圏エリアから利用可能エリアを導出し、新たに導出された利用可能エリア情報を格納することによりエリア情報DB22を更新する。なお、他サービス利用要求に対する利用許可応答はすでに送信されているので、この場合は利用許可応答は送信されない。このような構成とすれば、利用可能エリアを認証要求端末30の在圏エリアに合わせて常に最新化することができると共に、サービス検証システム10aは、再度他サービス要求を受信した際に利用許可メッセージ状態DB13を更新すればよく、接続中のすべての認証要求端末30の在圏エリアを監視しなくても良いので、サービス検証システム10の負担を軽減することができる。

【0084】

時間情報DB24は、第2のサービスを利用可能な時間に関する利用可能時間情報を格納するデータベースである。図9は、時間情報DB24に格納されたデータの例を示す図である。時間情報DB24には、「利用許可ID」「利用可能時間」の各情報が格納されている。「利用許可ID」は、利用許可メッセージを特定するための識別情報であり、利用許可メッセージ状態DB13に格納されたものと同じである。「利用可能時間」は、第2のサービスを利用できる時間に関する情報であり、この利用可能時間内にサービス利用端末から第2のサービスの利用要求メッセージを受信しなければ、サービスを提供しない。ここでは、利用可能時間情報は、利用許可IDに関連付けられているが、必ずしもこのようなデータ構造とする必要はなく、例えば認証要求端末30の識別情報などと関連付けて格納することとしても良いし、他の情報とは独立して格納することとしても良い。

【0085】

時間情報更新手段23は、時間情報DB24を更新する機能を有する。時間情報更新手段23は、他サービス利用可否判定手段17によってサービスBを利用可能と判定した場合に、サービスBを利用可能とする利用可能時間を設定する。例えば、他サービスの利用要求に対する判定の時点から開始して10分後までを利用可能時間として設定することもできるし、サービスBについては5分間、サービスBとは異なるサービスCについては10分間というようにサービス毎に利

用可能時間を設定することもできる。そして、時間情報更新手段 23 は、設定された利用可能時間情報をエリア情報 DB 22 に格納する。

【0086】

次に、第 2 実施形態に係るサービス検証ネットワークシステムの動作について図 10 を参照しながら説明し、併せて、第 2 実施形態に係るサービス提供方法について説明する。

【0087】

最初に、認証要求端末 30 は、サービス A を利用するための認証を行う (S10)。このステップは、第 1 実施形態における認証のステップと同じである (図 6 参照)。

【0088】

次に、認証要求端末 30 は、サービス A と異なるサービス B の利用要求をサービス検証システム 10 に送信する (S20)。サービス検証システム 10 は、認証要求端末 30 から送信される他サービス利用要求を受信する (S22) と、認証要求端末 30 のユーザがサービス B を利用可能であるか否か判定する (S24)。ここでは、サービス B を利用可能と判定されたものとする。サービス B を利用可能と判定されると、サービス検証システム 10 は、このユーザに対するサービス B の利用許可を識別する利用許可 ID を与え、利用許可メッセージ状態 DB 13 を更新する (S26)。利用許可メッセージは、最初、使用可能 (図 4 では「○」で示す) の状態で追加される。

【0089】

続いて、サービス検証システム 10 a は、エリア情報更新手段 21 によって認証要求端末 30 の在圏エリアから、第 2 のサービスを利用可能な利用可能エリア情報を導出し、エリア情報 DB 22 に格納する。また、サービス検証システム 10 a は、時間情報更新手段 23 によって第 2 のサービスを利用可能な利用可能時間情報を設定し、時間情報 DB 24 に格納する。

【0090】

次に、サービス検証システム 10 は、利用要求に係るサービス B について利用許可メッセージに基づく利用許可応答を認証要求端末 30 に送信する (S28)

。認証要求端末30は利用許可応答を受信する(S30)と、受信した利用許可応答をサービス利用端末40に伝達する。本実施形態においては、認証要求端末30はサービス利用端末40との間で無線通信可能であるとし、認証要求端末30がサービス利用端末40に無線によって利用許可応答を送信し(S32)、サービス利用端末40が利用許可応答を受信するものとする(S34)。

【0091】

サービス利用端末40は、認証要求端末30から送信された利用許可応答を受信する(S34)と、利用許可応答に基づいてサービスBの利用を要求するメッセージを作成し、サービス利用端末40は、作成したメッセージをサービス検証システム10に送信する(S36)。サービス検証システム10は、サービス利用端末40から送信されたメッセージを受信し(S38)、受信したメッセージに基づいている利用許可メッセージを解析し、利用許可メッセージ状態DB13からメッセージ状態情報を検索する(S40)。続いて、受信したメッセージに基づいている利用許可メッセージが使用可能な状態か否か、さらに受信したメッセージ自体が正しく構成されているか否かの整合性を利用許可メッセージ状態DB13に基づいて判定する。第2実施形態に係るサービス検証システム10aは、エリア情報DB22から利用可能エリアの情報を検索し、時間情報DB24から利用可能時間の情報を検索する(S43)。そして、サービス検証システム10aは、サービス提供可否判定手段19によって、サービス利用端末40がエリア情報DB22に格納された利用可能エリア情報で示されるエリア内に存在するか否かを判定する。さらに、サービス提供可否判定手段19は、第2のサービスの利用要求メッセージを受信した時刻が、時間情報DB24に格納された利用可能時間内であるか否かを判定する。これらの判定により、サービス利用端末が利用可能エリア内にあって、さらに利用可能時間内にメッセージを送信してきた場合に、サービス提供可否判定手段19は、第2のサービスを利用可能と判定する(S46)。サービスを提供可能である場合には、利用許可メッセージ状態解除手段20は利用許可メッセージ状態DB13に格納された利用許可メッセージの状態を使用可能な状態から使用できない状態にし、サービスBの利用可能状態を解除する。

【0092】

次に、サービス検証システム10は利用許可応答をサービス利用端末40に送信し(S48)、サービス利用端末40はサービス提供端末から送信された利用許可応答を受信し(S50)、サービスBを利用することが可能となる。以上で、本実施形態に係るサービス検証ネットワークシステムの動作フローは終了する。

【0093】

第2実施形態に係るサービス検証システム10aは、第1実施形態に係るサービス検証システム10と同様に、サービスAを提供するサービス検証システム10aにおいて、新たなサービスBを提供する場合に、サービスBを利用可能なユーザを認証する認証手段16を新たに構築しなくても、サービスAの認証手段16による認証結果を利用することで、低コストかつ短時間でサービス検証システム10aを準備することができる。

【0094】

さらに、第2実施形態に係るサービス検証システム10aは、エリア情報DB22に利用可能エリア情報を格納し、当該利用可能エリアでのサービス利用を許可するため、サービスを利用することができるエリアを限定し、不正利用の機会を少なくしてセキュリティを向上させることができる。また、時間情報DB24に利用可能時間情報を格納し、当該時間内においてサービス利用を許可するため、サービスを利用することができる時間を限定し、不正利用の機会を少なくしてセキュリティを向上させることができる。

【0095】

また、第2実施形態に係るサービス提供方法は、第1実施形態に係るサービス提供方法と同様に、サービスAを提供するサービス検証システム10において、新たなサービスBを提供する場合に、サービスBを利用可能なユーザを認証する認証手段16を新たに構築しなくても、サービスAの認証手段16による認証結果を利用することで、低コストかつ短時間でサービス検証システム10を準備することができる。

【0096】

(第3実施形態)

次に、本発明の第3実施形態に係るサービス検証ネットワークシステムについて説明する。第3実施形態に係るサービス検証ネットワークシステムは、第1実施形態に係るサービス検証ネットワークシステム1と基本的な構成は同じである(図1参照)が、サービス検証システム10から送信される利用許可応答に含まれる情報と、サービス利用端末40から送信される利用要求に含まれる情報とが、第1実施形態に係るサービス検証ネットワークシステム1とは異なる。以下、第1実施形態に係るサービス検証ネットワークシステム1との相違点について述べる。

【0097】

また、第3実施形態に係るサービス検証システム10の通信手段14は、他サービスの利用要求に対して、当該他サービスを利用可能である場合には利用許可応答を送信するが、その利用許可応答は、利用許可メッセージに関する情報に加えて、利用可能エリア情報及び利用可能時間情報に基づいている。これに伴い、第3実施形態に係るサービス利用端末40の第2メッセージ送信手段41は、利用許可メッセージに関する情報に加えて、利用可能エリア情報及び利用可能時間情報に基づく利用要求のメッセージを作成し、サービス検証システム10に送信する機能を有する。

【0098】

次に、第3実施形態に係るサービス検証ネットワークシステムの動作について図11を参照しながら説明し、併せて第3実施形態に係るサービス提供方法について説明する。

【0099】

第3実施形態に係るサービス検証ネットワークシステムの動作は、基本的には第1実施形態に係るサービス検証ネットワークシステム1の動作と同じであるので、第1実施形態に係るサービス検証システム10の動作と異なる点について説明する。ステップS28において、サービスBの利用許可応答を送信する際に、利用許可メッセージ、利用可能エリア情報、及び利用可能時間情報に基づく利用許可応答を認証要求端末30に送信する。そして、ステップS34において利用

許可応答を受信したサービス利用端末40は、ステップS36において利用要求メッセージを送信する際に、利用許可メッセージ、利用可能エリア情報、及び利用可能時間情報に基づく利用要求応答に基づいてメッセージを作成し、サービス検証システム10に送信する(S36)。サービス検証システム10は、サービス利用端末40から送信されたメッセージを受信する(S38)と、そのメッセージが基づいている利用許可メッセージの状態と、受信したメッセージ自体が正しく構成されているか否かの整合性を利用許可メッセージ状態DB13に基づいて判定する。ここで、利用要求メッセージが基づいている利用許可メッセージが「A102」であるとする、利用許可メッセージ状態DB13を参照して状態「O」であることがわかる。また、サービス利用端末40から受信した利用要求メッセージが基づいている利用要求エリア情報、利用要求時間情報を解析し(S44)、サービス利用端末40の在圏エリアが利用可能エリアに含まれているか否か、また、利用要求メッセージの受信時刻が利用可能時間内であるか否かを判定し、サービスBの提供可否を判定する(S46)。

【0100】

第3実施形態に係るサービス検証ネットワークシステム及び方法は、第1実施形態に係るサービス検証ネットワークシステム1及び方法と同様に、サービスAの認証結果を用いてサービスBを利用可能とすることにより、サービスBのために新たな認証手段を設ける必要がなく、低コストかつ短時間でサービスBを提供するサービス検証システム10を準備することができる。

【0101】

また、第3実施形態に係るサービス検証ネットワークシステムでは、サービス検証システム10の利用許可メッセージ状態DB13が利用可能エリア情報や利用可能時間情報を有しない構成であるので、サービス検証システム10で格納するデータ量を減らすことができる。

【0102】

以上、本発明のサービス検証ネットワークシステムについて、実施形態を挙げて詳細に説明したが、本発明は上記実施形態に限定されるものではない。

【0103】

例えば、上記第2実施形態においては、サービスBを利用可能か否か判定するに際して、利用可能エリア情報や利用可能時間情報をも用いているが、いずれか一方のみを用いることとしても良い。このようにすれば、セキュリティの向上を図りつつ、判定のステップを減らして提供可否判定処理の速度を高めることができる。

【0104】

また、サービス利用端末は、追加情報として自身の端末を識別する識別情報を格納した識別情報格納手段をさらに備えることとし、この識別情報と認証要求端末30が受信した利用許可応答とに基づいて、サービスBの利用要求のメッセージを作成し、サービス検証システム10に送信することとしても良い。このような構成を採用すれば、第2のサービスを利用可能な端末を制限できるので、セキュリティを向上させることができる。

【0105】

また、サービス利用端末は、追加情報として認証情報を格納した認証情報格納手段をさらに備えることとし、この認証情報と認証要求端末30が受信した利用許可応答とに基づいて、サービスBの利用要求のメッセージを作成し、サービス検証システム10に送信することとしても良い。このような構成を採用すれば、第2のサービスをより安全に提供することができる。

【0106】

【発明の効果】

本発明によれば、認証手段による認証によって認証要求端末のユーザが正規ユーザであることを認証した状態で、そのユーザが第2のサービスを利用可能か判定するので、第1のサービスの認証結果を利用して、第2のサービスについては認証を省略することができる。そして、利用許可を識別する利用許可メッセージを格納すると共に、利用許可メッセージに基づく利用許可応答を認証要求端末に送信し、認証要求端末から知得した利用許可応答に基づく利用要求メッセージが第2の端末から送信された場合には、その利用要求メッセージに基づいている利用許可メッセージのメッセージ状態情報を利用許可メッセージ状態DBに基づいて検証して、使用可能な状態であった場合には第2の端末に対して第2のサービ

スを提供する。これにより、サービス検証システムは利用許可メッセージの状態を検証するのみで、第2の端末のユーザを特定するまでもなく、第2の端末にサービスを提供可能か否かを判定することができる。以上のように、第2のサービスの利用に際し、第1のサービスの認証結果を用いることにより、第2のサービスを提供する際に新たな認証手段を最初から作り上げる必要はなく、コストや設計時間を削減することができる。

【図面の簡単な説明】

【図1】

実施形態に係るサービス検証ネットワークシステムの構成を示すブロック図である。

【図2】

認証情報DBに格納されたデータ項目の例を示す図である。

【図3】

利用可能サービス情報DBに格納されたデータ項目の例を示す図である。

【図4】

利用許可メッセージ状態DBに格納されたデータ項目の例を示す図である。

【図5】

第1実施形態に係るサービス検証ネットワークシステムの動作を示すフローチャートである。

【図6】

認証処理を示すフローチャートである。

【図7】

第2実施形態に係るサービス検証システムの構成を示すブロック図である。

【図8】

エリア情報DBに格納されたデータの例を示す図である。

【図9】

時間情報DBに格納されたデータの例を示す図である。

【図10】

第2実施形態に係るサービス検証ネットワークシステムの動作を示すフローチャートである。

ャートである。

【図 11】

第2実施形態に係るサービス検証ネットワークシステムの動作を示すフローチャートである。

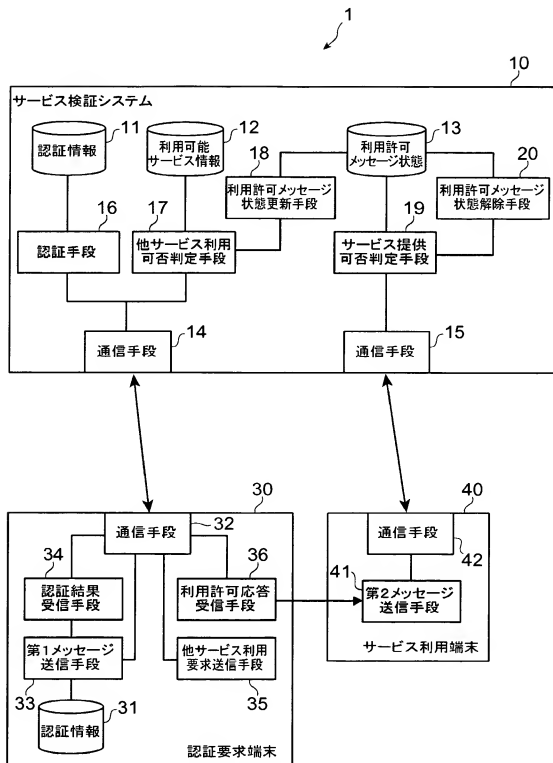
【符号の説明】

1…サービス検証ネットワークシステム、10…サービス検証システム、11…認証情報DB、12…利用可能サービス情報DB、13…利用許可メッセージ状態DB、14、15…通信手段、16…認証手段、17…他サービス利用可否判定手段、18…利用許可メッセージ状態更新手段、19…サービス提供可否判定手段、30…認証要求端末、31…認証情報DB、32…通信手段、33…認証情報送信手段、34…認証結果受信手段、35…他サービス利用要求送信手段、26…利用許可応答受信手段、40…サービス利用端末、41…利用要求送信手段、42…通信手段。

【書類名】

図面

【図 1】



【図 2】

11

ID	パスワード	シェアード シークレット	秘密鍵	公開鍵	認証方法
U100	—	—	—	—	—
U101	—	—	—	—	—
U102	—	—	—	—	—
...

【図 3】

12

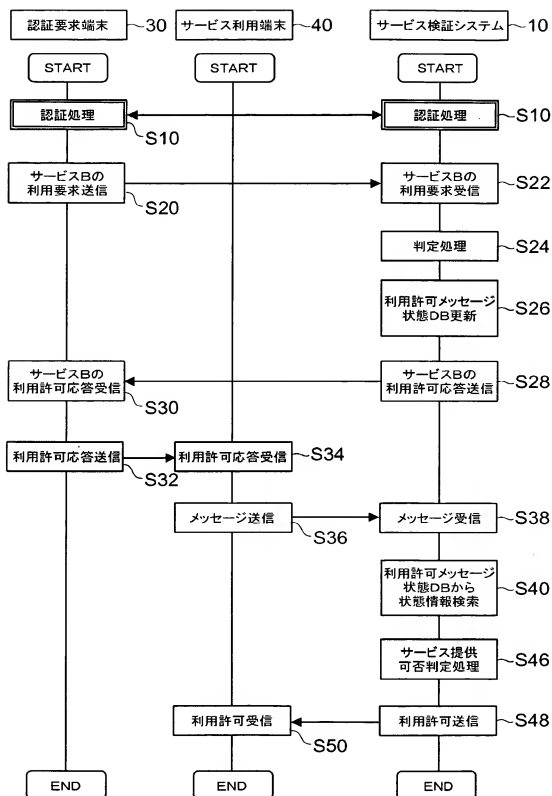
ID	サービスB
U100	○
U101	×
U102	○
⋮	⋮

【図 4】

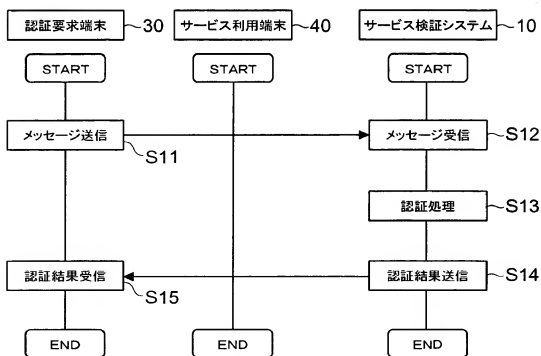
13

利用許可ID	状態
A100	○
A101	×
A102	○
⋮	⋮

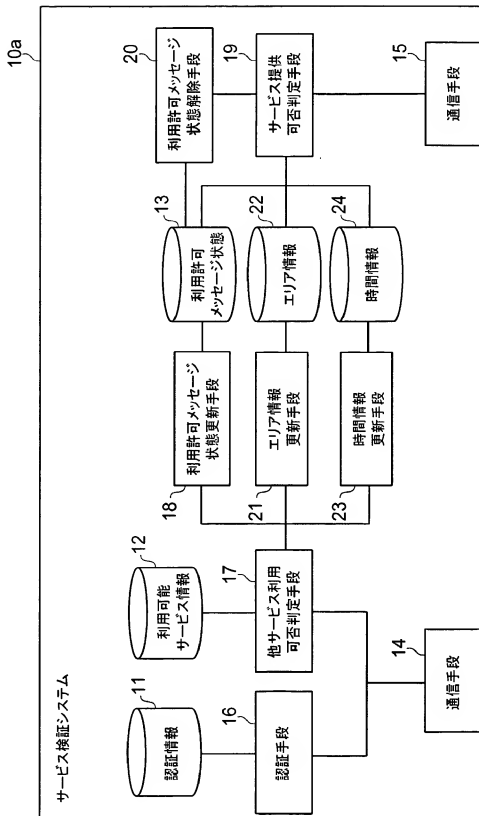
【図 5】



【図 6】



【図 7】



【図 8】

22

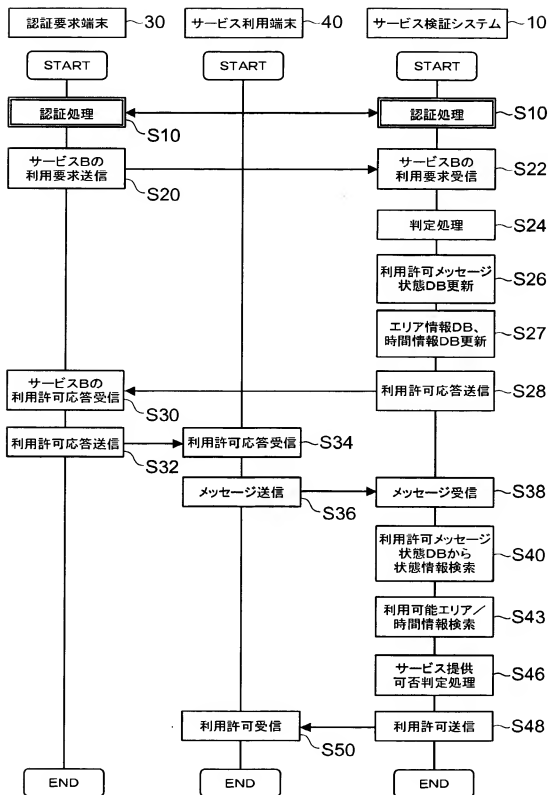
利用許可ID	利用可能エリア
A100	エリアA
A101	エリアB
A102	エリアC
⋮	⋮

【図9】

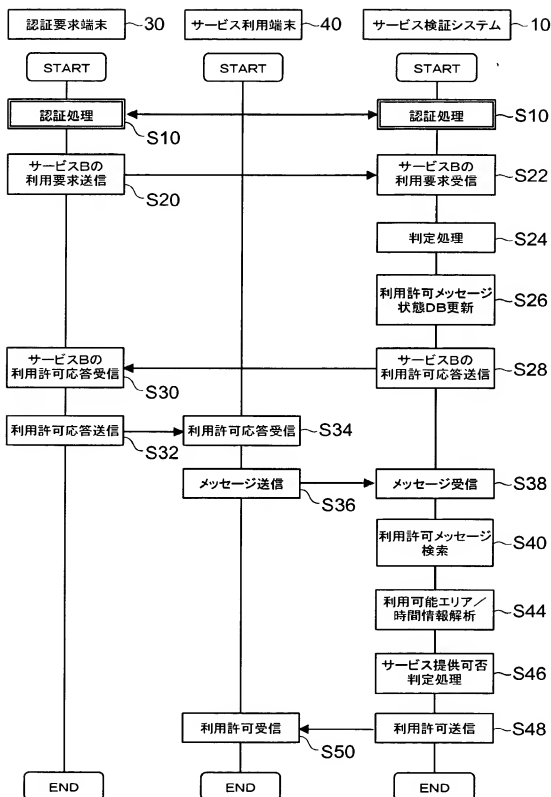
24

利用許可ID	利用可能時間
A100	10:00~10:05
A101	10:02~10:07
A102	10:05~10:10
⋮	⋮

【図 10】



【図 11】



【書類名】 要約書**【要約】**

【課題】 コスト上昇を抑制することができるサービス提供方法を提供する。

【解決手段】 本発明に係るサービス提供方法は、サービスA及びBを提供するサービス提供方法であって、サービスAを利用可能とするために認証要求端末30のユーザの認証を行い、サービスAについての認証がなされた状態で、そのユーザがサービスBを利用できるか判定する。サービスBを利用可能と判定された場合には、利用許可メッセージを格納すると共に、認証要求端末30にサービスBの利用許可メッセージに基づく利用許可応答を送信する。そして、サービス利用端末40から送信される利用要求メッセージに基づいている利用許可メッセージを検証し、使用可能な状態であれば、サービス利用端末40に対してサービスBを利用可能とする。サービスAについての認証結果を利用することでサービスBについて新たな認証手段を設ける必要がなく、コスト低減に繋がる。

【選択図】 図5

特願 2002-302102

出願人履歴情報

識別番号

[392026693]

1. 変更年月日
[変更理由]

2000年 5月19日

名称変更

住所変更

住 所
氏 名

東京都千代田区永田町二丁目11番1号
株式会社エヌ・ティ・ティ・ドコモ